Nonlinarity of Boolean functions and hyperelliptic curves

Eric Férard[*], François Rodier[†]

Boolean functions is an important tool in computer sciences. It is especially useful in private key cryptography for designing stream ciphers. For security reasons, and also because Boolean functions need also to have other properties than nonlinearity such as balancedness or high algebraic degree, it is important to have the possibility of choosing among many Boolean functions, not only bent functions, that is functions with the highest possible non linearity, but also functions which are close to be bent in the sense that their nonlinearity is close to the nonlinearity of bent functions. For m odd, it would be particularly interesting to find functions with nonlinearity larger than the one of quadratic Boolean functions (called *almost optimal* in [1]). This has been done for instance in the work of Patterson and Wiedemann [9] and also of Langevin-Zanotti [4].

Let $q = 2^m$ and $\mathbf{F}_{2^m}$ assimilated as a vector space to $\mathbf{F}_2^m$. In this talk, we want to study functions of the form $\mathrm{Tr}\, G(x)$, where G is a polynomial on $\mathbf{F}_{2^m}$ and Tr the trace of $\mathbf{F}_{2^m}$ over $\mathbf{F}_2$.

For m even, many people got interested in finding bent functions of this form. To only mention the case of monomials, one can get the known cases (Gold , Dillon/Dobbertin, Niho exponents) in the paper of Leander [5].

For m odd, one might have expected that among the functions $f : x \longrightarrow \mathrm{Tr}\, G(x)$ where G is a polynomial of degree 7, there are some functions which are close to being bent in the previous sense. This happens not to be the case, but we will show that for m odd such functions have rather good nonlinearity or autocorrelation properties. We use for that recent results of Maisner and Nart [7] about zeta functions of supersingular curves of genus 2.

[*]Université de Polynésie française, Tahiti; e-mail ferard@upf.pf

[†]Institut de Mathématiques de Luminy – C.N.R.S. 163 avenue de Luminy, Case 907, Marseille Cedex 9, France; e-mail rodier@iml.univ-mrs.fr

On the other hand, vectorial Boolean functions are used in cryptography to construct block ciphers. An important criterion on these functions is a high resistance to the differential cryptanalysis. Nyberg [8] has introduced the notion of almost perfect nonlinearity (APN) to study differential attacks. We relate this notion to the notion above, and we will give some criterion for a function not to be almost perfect nonlinear.

1 Preliminaries

1.1 Boolean functions

Let m be a positive integer and $q = 2^m$.

Definition 1.1 *A Boolean function with m variables is a map from the space $V_m = \mathbf{F}_2^m$ into $\mathbf{F}_2$.*

A Boolean function is linear if it is a linear form on the vector space V_m. It is affine if it is equal to a linear function up to addition of a constant.

1.2 Nonlinearity

Definition 1.2 *We call nonlinearity of a Boolean function $f : V_m \longrightarrow \mathbf{F}_2$ the distance from f to the set of affine functions with m variables:*

$$nl(f) = \min_{h \text{ affine}} d(f, h)$$

where d is the Hamming distance.

One can show that the nonlinearity is equal to

$$nl(f) = 2^{m-1} - \frac{1}{2}\|\widehat{f}\|_\infty$$

where

$$\|\widehat{f}\|_\infty = \sup_{v \in V_m} \Big| \sum_{x \in V_m} \chi\left(f(x) + v \cdot x\right) \Big|,$$

where $v \cdot x$ denote the usual scalar product in V_m and $\chi(f) = (-1)^f$. It is the maximum of the Fourier transform of $\chi(f)$ (the Walsh transform of f):

$$\widehat{f}(v) = \sum_{x \in V_m} \chi\left(f(x) + v \cdot x\right).$$

Parseval identity can be written

$$\|\widehat{f}\|_2^2 = \frac{1}{q}\sum_{v\in V_m}\widehat{f}(v)^2 = q$$

and we get, for f a Boolean function on V_m:

$$\sqrt{q} \leq \|\widehat{f}\|_\infty \leq q.$$

1.3 The sum-of-square indicator

Let f be a Boolean function on V_m. Zhang and Zheng introduced the *sum-of-square indicator* [14], as a measure of the *global avalanche criterion*:

$$\sigma_f = \frac{1}{q}\sum_{x\in V_m}\widehat{f}(x)^4 = \|\widehat{f}\|_4^4.$$

We remark that

$$\|\widehat{f}\|_2 \leq \|\widehat{f}\|_4 \leq \|\widehat{f}\|_\infty. \tag{1}$$

Hence the values of $\|\widehat{f}\|_4$ may be considered as a first approximation of $\|\widehat{f}\|_\infty$ and in some cases they may be easier to compute. The relationship of this function with non-linearity was studied by A. Canteaut et al.[1].

2 The functions $f : x \longrightarrow \mathrm{Tr}\,(G(x))$ where G is a polynomial

2.1 Divisibility of $\|\widehat{f}\|_\infty$

Let $G(x)$ be the polynomial $\sum_{i=0}^{s} a_i x^i$ with coefficients in $\mathbf{F}_q$ and f the Boolean function $\mathrm{Tr}\circ G$.

Definition 2.1 *The binary degree of G is the maximum value of $\sigma(i)$ for $0 \leq i \leq s$, where $\sigma(i)$ is the sum of the binary digits of i.*

One has the following proposition, due to C. Moreno and O. Moreno [6].

Proposition 2.1 *Let G be a polynomial with coefficients in $\mathbf{F}_q$ and binary degree d. Then $\|\widehat{f}\|_\infty$ is divisible by $2^{\lceil \frac{m}{d} \rceil}$.*

2.2 Case where G is a polynomial of binary degree 2

The $\|\widehat{f}\|_\infty$ are multiple of $2^{\lceil \frac{m}{2} \rceil}$. Therefore, if m is even $\|\widehat{f}\|_\infty$ is a multiple of $q^{1/2}$, and if m is odd, of $\sqrt{2q}$. In particular, if m is odd, the spectral amplitude is higher or equal to $\sqrt{2q}$ which is equal to that of the quadratic Boolean functions, of the maximum rank.

3 The functions $f : x \longrightarrow \mathrm{Tr}\,(G(x))$ where G is a binary polynomial of degree 3

One simply will study the case where G is a binary polynomial of degree 2 to which one adds a monomial of degree 7:

$$G = a_7 x^7 + \sum^{s} b_i x^{2^i+1}$$

where $a_7 \neq 0$ a polynomial of degree 7 with coefficients in k. We would like to evaluate $\|\widehat{f}\|_4$ on $\mathbf{F}_{2^m}$, for $f(x) = \mathrm{Tr}\,(G(x))$ where Tr indicates the function trace of $\mathbf{F}_q$ on $\mathbf{F}_2$:

$$\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{2^i}.$$

One obtains the simple expression of $\|\widehat{f}\|_4$ (cf [10, 11]):

$$\|\widehat{f}\|_4^4 = \sum_{x_1+x_2+x_3+x_4=0} \chi\left(f(x_1)+f(x_2)+f(x_3)+f(x_4)\right) = q^2 + \sum_{\alpha \in k^*} X_\alpha$$

with

$$X_\alpha = \Big(\sum_{x \in k} \chi \circ \mathrm{Tr}\left(G(x)+G(x+\alpha)\right) \Big)^2.$$

To compute X_α, one can remark that the curve of equation $y^2 + y = G(x+\alpha) + G(x)$ is isomorphic to

$$\begin{aligned} y^2 + y = {} & G(\alpha) + \\ & + (a_7\alpha^6 + a_7^{1/4}\alpha^{3/4} + a_7^{1/2}\alpha^{5/2} + \sum (b_i\alpha)^{2^{-i}} + \sum b_i \alpha^{2^i})x + \\ & + (a_7\alpha^4 + a_7^{1/2}\alpha^{1/2})x^3 + a_7\alpha^2 x^5 \end{aligned}$$

which is an equation of a curve C_1 of genus 2 for $\alpha \neq 0$. One has

$$X_\alpha = (\#C_1 - q - 1)^2.$$

To compute X_α, we will need results of Van der Geer - van der Vlugt and of Maisner - Nart.

3.1 Van der Geer and van der Vlugt theory

Let C_1 the curve with affine equation:

$$C_1 : y^2 + y = ax^5 + bx^3 + cx + d$$

with $a \neq 0$. Let R be the linearized polynomial $ax^4 + bx^2 + c^2x$. The map

$$\begin{array}{rcl} Q : k & \to & \mathbf{F}_2 \\ x & \mapsto & \mathrm{Tr}(xR(x)) \end{array}$$

is the quadratic form associated to the symplectic form

$$\begin{array}{rcl} k \times k & \longrightarrow & \mathbf{F}_2 \\ (x,y) & \mapsto & < x, y >_R = \mathrm{Tr}(xR(y) + yR(x)). \end{array}$$

The number of zeros of Q determines the number of points of C_1:

$$\#C_1(k) = 1 + 2\#Q^{-1}(0).$$

Let W be the radical of the symplectic form $<,>_R$, and w be its dimension over $\mathbf{F}_2$. The codimension of the kernel V of Q in W is equal to 0 or 1.

Theorem 3.1 *(van der Geer - van der Vlugt [13])*
If $V \neq W$, then $\#C_1(k) = 1 + q$.
If $V = W$, then $\#C_1(k) = 1 + q \pm \sqrt{2^w q}$.

3.2 Values of X_α

In [3], we study the factorization of P which determines V and W (see Maisner-Nart [7]). Thanks to the work of van der Geer - van der Vlugt, we can compute the number of points of the curves $y^2 + y = G(x + \alpha) + G(x)$.

Proposition 3.1 *Suppose that m is odd. Then*

$$X_\alpha = 0 \quad or \quad 2q \quad or \quad 8q.$$

Let $\ell = a_7^{-1/3}\alpha^{-7/3}$. Then

$X_\alpha = 8q$ *if and only if*

$$\mathrm{Tr}\,\ell = 0 \quad , \quad \ell = v + v^4 \quad with \quad \mathrm{Tr}\,v = 0 \quad ,$$
$$\mathrm{Tr}\left(\frac{(a+c)\alpha}{\lambda}v^3\right) = 1 \quad , \quad \mathrm{Tr}\left(\frac{(a+c)\alpha}{\lambda}(v+v^2)\right) = 1 \quad ;$$

$X_\alpha = 2q$ *if and only if* $\mathrm{Tr}\,\ell = 1$;

$X_\alpha = 0$ *in the remaining cases.*

4 Evaluation of $\|\widehat{f}\|_4^4$

Proposition 4.1 *The value of* $\|\widehat{f}\|_4^4$ *on* $\mathbf{F}_{2^m}$ *when* m *is odd and* $f(x) = \mathrm{Tr}\,(G(x))$ *is such that*

$$|\|\widehat{f}\|_4^4 - 3q^2| \leq 185.2^{s-1}q^{3/2}.$$

Proof

One can evaluate the number of α which gives each case of the preceding proposition. The proves of these evaluations are linked with the computations of exponential sums over the curve $v + v^4 = \gamma x^7$. We get

$$\begin{aligned} \left|\#\{\alpha \mid X_\alpha = 8q\} - \frac{1}{8}\right| &\leq 23.2^{s-1}q^{1/2} \\ \left|\#\{\alpha \mid X_\alpha = 2q\} - \frac{1}{2}\right| &\leq 3q^{1/2} + 1 \end{aligned}$$

One deduce easily the evaluation of $\|\widehat{f}\|_4^4$. The details of the proof will appear in [3].

Remark 4.1 *This result is to be compared with proposition 5.6 in [10] where the distribution of* $\|\widehat{f}\|_4^4$ *for all Boolean function is shown to be concentrated around* $3q^2$*.*

5 Bound for $\|\widehat{f}\|_\infty$

From the theorem, we can deduce some lower bounds for $\|\widehat{f}\|_\infty$.

Proposition 5.1 *For the functions* $f : x \longrightarrow \mathrm{Tr}\,(G(x))$ *on* $\mathbf{F}_{2^m}$ *where* G *is the polynomial* $G = a_7x^7 + \sum^s b_i x^{2^i+1}$ *and* m *is odd one has, for* $m \leq 11+2s$*:*

$$\sqrt{2q} \leq \|\widehat{f}\|_\infty.$$

For $m \geq 15 + 2s$*, one has moreover:*

$$\sqrt{2q} < \|\widehat{f}\|_\infty.$$

Proof

The evaluation of the number of α such that $\mathrm{Tr}\,\ell = 1$ in proposition 3.1 gives:

$$2q^2 - 6q^{3/2} \leq \|\widehat{f}\|_4^4.$$

As it is easy to show that

$$\|\widehat{f}\|_4^4 \leq q\|\widehat{f}\|_\infty^2$$

we get $2q - 6q^{1/2} \leq \|\widehat{f}\|_\infty^2$ whence the result, as $\|\widehat{f}\|_\infty$ is divisible by $2^{\lceil m/3 \rceil}$.

The second inequality is a consequence of theorem 4.1.

Remark 5.1 *So f is not almost optimal (in the sense of [1]), for $m \geq 15 + 2s$.*

6 APN Functions

Let us consider a function $G : \mathbf{F}_q \longrightarrow \mathbf{F}_q$.

Definition 6.1 *The function G is said to be APN (almost perfect nonlinear) if for every $a \in \mathbf{F}_q^*$ and $b \in \mathbf{F}_q$, there exists at most 2 elements of $\mathbf{F}_q$ such that $G(z + a) + G(z) = b$.*

Proposition 6.1 *The function*

$$\begin{array}{rccl} G: & \mathbf{F}_q & \longrightarrow & \mathbf{F}_q \\ & x & \mapsto & a_7 x^7 + \sum_0^s b_i x^{2^i+1} \end{array}$$

is not APN for $m \geq 13 + 2s$.

Proof

For $\gamma \in \mathbf{F}_q$, consider the function $f_\gamma(x) = \mathrm{Tr}(G(\gamma x))$. The proposition follows from proposition 4.1 and the following result from Chabaud-Vaudenay [2].

Proposition 6.2 *One has* $\sum_{\gamma \in k^*} \sigma(f_\gamma) \geq 2q^2(q-1)$.

The function G is APN if and only if the **equality is true.**

For $s \leq 2$, one can even say more. The following theorem [12] proves that the function G is not APN for $m \geq 11$.

Theorem 6.1 *Let G be a polynomial from $\mathbf{F}_{2^m}$ to $\mathbf{F}_{2^m}$, d its degree. Let us suppose that the curve X_∞ of equation*

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is smooth. Then if $m \geq 6$ and $d < q^{1/6} + 3.9$, G is not APN.

References

[1] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine *Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions,* Advances in cryptology, EUROCRYPT 2000 (Bruges), 507–522, Lecture Notes in Comput. Sci., Vol. 1807, Springer, Berlin, 2000.

[2] Chabaud, Florent; Vaudenay, Serge *Links between differential and linear cryptanalysis.* De Santis, Alfredo (ed.), Advances in cryptology - EUROCRYPT '94. Workshop on the theory and application of cryptographic techniques, Perugia, Italy, May 9-12, 1994. Proceedings. Berlin: Springer-Verlag. Lect. Notes Comput. Sci. 950, 356-365 (1995).

[3] E. Férard, F. Rodier, *Nonlinearity of some Boolean functions*, work in preparation.

[4] P. Langevin, J-P. Zanotti, *A note on the counter-example of Patterson-Wiedemann*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), 214–219, Springer, Berlin, 2002.

[5] G. Leander *Monomial Bent Functions*, WCC05 (International Workshop on Coding and Cryptography, March 2005, Bergen, Norway), Oyvind Ytrehus, Springer-Verlag New York.

[6] C. Moreno and O. Moreno *The MacWilliams-Sloane conjecture on the tightness of the Carlitz- Uchiyama bound and the weights of duals of BCH codes,* IEEE Trans. Inf. Theory 40, No.6, 1894-1907 (1994).

[7] D. Maisner and E. Nart, *Zeta functions of supersingular curves of genus 2*, arXiv:math.NT/0408383

[8] Nyberg, Kaisa Differentially uniform mappings for cryptography. Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993), 55–64, Lecture Notes in Comput. Sci., 765, Springer, Berlin, 1994.

[9] N. Patterson and D. Wiedemann, *The covering radius of the* $(2^{15}, 16)$ *Reed-Muller code is at least* 16 276, IEEE Trans. Inform. Theory 29, no. 3 (1983), 354-356.

[10] F. Rodier, *Sur la non-linéarité des fonctions booléennes*, Acta Arithmetica, vol 115, (2004), 1-22, preprint: arXiv: math.NT/0306395.

[11] F. Rodier, *On the nonlinearity of Boolean functions*, Proceedings of WCC2003, Workshop on coding and cryptography 2003 (D. Augot, P. Charpin, G. Kabatianski eds), INRIA (2003), pp. 397-405.

[12] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*; ArXiv: math.AG/0605232, 2006.

[13] G. van der Geer, M. van der Vlugt, *Reed-Muller codes and supersingular curves. I*, Compositio Math. 84, (1992), 333-367.

[14] Xian-Mo Zhang and Yuliang Zheng, *GAC —the Criterion for Global Avalanche Characteristics of Cryptographic Functions*, Journal of Universal Computer Science, vol. 1, no. 5 (1995), 316-333